(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 878 907 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
18.11.1998 Bulletin 1998/47

(51) Int. Cl.[6]: **H03K 3/84**

(21) Application number: **98108506.1**

(22) Date of filing: **11.05.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **16.05.1997 GB 9710056**

(71) Applicant: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Stout, Graham**
  Giffnock, Glasgow, Scotland G46 6PP (GB)
- **Lin, Bo**
  Stewartfield, East Kilbride (GB)
- **Mcallister, Stephen**
  Greenhills, East Kilbride, Glasgow (GB)

(74) Representative:
Gibson, Sarah Jane et al
Motorola
European Intellectual Property Operations
Midpoint
Alencon Link
Basingstoke, Hampshire RG21 7PL (GB)

(54) Random number generator arrangement and method of generation thereof

(57) A random number generator (110) comprises: a first oscillator arrangement (112, 114) for producing a varying waveform output signal at a first frequency; a second oscillator arrangement (116, 118) coupled to the output of the first oscillator arrangement so that the frequency of the second oscillator means is controlled by the output of the first oscillator arrangement, for producing a pulse train output representative of a random number; and an adjustment arrangement (120, 122) coupled between the output of the first oscillator arrangement and the second oscillator arrangement for adjusting by a variable amount the frequency of the second oscillator means.

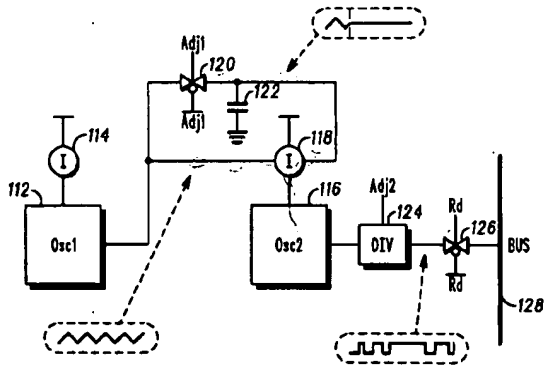

FIG. 2

EP 0 878 907 A2

Description

FIELD OF THE INVENTION

This invention relates generally to random number generation.

BACKGROUND OF THE INVENTION

Random number generation is required in a range of applications, and particularly though not exclusively in security applications where a random number is used in the generation of an encoding or encryption key. As used herein, it is to be understood that the term random number covers both numbers which are truly or mathematically random as well as numbers which approximate to or have a degree of randomness (typically called pseudo random numbers).

It is well known that a random number generator can be designed by cascading two or more independent oscillators. This can be done in software or in hardware.

Referring now to FIG. 1 of the accompanying drawings, in a typical hardware implementation of a cascaded-oscillator random number generator circuit 10 a first oscillator 12 is a relaxation oscillator which charges and discharges a capacitor (not shown) from a first, fixed current source 14 to produce a saw-tooth waveform output at a first frequency. A second oscillator 16 is also a relaxation oscillator which charges and discharges a capacitor (not shown) from a second, voltage-controlled current source 18. The second current source 18 which supplies the second oscillator 16, is modulated by the saw-tooth waveform output from the first oscillator 12. The output of the second oscillator 16 is thus a pulse train representing a random number which is gated, via a transmission gate 20 controlled by a read signal Rd, onto a data bus 22.

It has been realised that in practice certain factors may reduce the randomness of the number produced by the circuit of FIG. 1. For example, the frequencies of the first and second oscillators will vary with variations in supply voltage and temperature. Thus, although the circuit output will be generally non-periodic, it may be possible to find a voltage where the oscillators "beat" in harmony, resulting in a periodic output.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a random number generator arrangement and method of generation thereof in which the above disadvantages are overcome or at least alleviated.

In accordance with a first aspect of the invention there is provided a random number generator arrangement as claimed in claim 1.

In accordance with a second aspect of the invention there is provided a method of generating a random number as claimed in claim 9.

BRIEF DESCRIPTION OF THE DRAWINGS

One random number generator arrangement and method of generation thereof will now be described, by way of example only, with reference to the accompanying drawings, in which:

FIG. 1 shows a block schematic diagram of a random number generator arrangement known in the prior art; and

FIG. 2 shows a random number generator arrangement incorporating the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Referring now to FIG. 2 of the accompanying drawings, a cascaded-oscillator random number generator 110 includes a first relaxation oscillator 112 which charges and discharges a capacitor (not shown) from a first, fixed current source 114 to produce a saw-tooth waveform output at a first frequency. A second relaxation oscillator 116 charges and discharges a capacitor (not shown) from a second, voltage-controlled current source 118. The second current source 118 is coupled at a first control input directly to the output of the first oscillator 112 to be modulated by the saw-tooth waveform output thereof. As will be discussed further below, the output of the first oscillator 112 is also coupled to a second control input of the second current source 118 via a transmission gate 120, which is controlled by the state of a software settable data bit (not shown), which controls an adjust signal Adj1. A storage capacitor 122 is connected between ground and a point between the transmission gate 120 and the second current source 118.

The output of the second oscillator 116 is coupled through a divider 124 and a transmission gate 126 (controlled by a read signal Rd) onto a data bus 128. The divide ratio of the divider 124 is selectable between unity and a predetermined, non-unity value by the state of a software settable data bit (not shown), which controls an adjust signal Adj2.

The random number generator 110 allows a user to select one of four settings of the two adjust bits described above to adjust the randomness of the random number produced thereby.

The adjustment bit which controls the divider 124 determines whether the output pulse train from the second oscillator 116 is divided by a predetermined ratio before being gated onto the data bus 128. It will be appreciated that such division of the output pulse train from the second oscillator 116 further 'randomises' the resultant number.

The adjustment bit which controls the transmission gate 120 acts as follows to 'randomise' the resultant number in a more fundamental way. The transmission

gate 120 and the storage capacitor 122 allow the user to adjust the second current source 118 by an analogue value determined by the point in time when the output saw-tooth waveform from the first oscillator 112 is sampled and held upon closure of the transmission gate 120. The user adjusts the randomness of the resultant number by 'blipping' or 'pulsing' the adjustment bit for the transmission gate 120 (i.e., setting the adjustment bit to a value, say '0' to open the transmission gate 120, then waiting for a predetermined time - set in software - before setting the adjustment bit to the opposite value, say '1', to close the transmission gate 120 and leave the sampled value of the output saw-tooth waveform from the first oscillator 112 at that instant stored on the capacitor 122). Thus, 'blipping' or 'pulsing' the adjust bit for the transmission gate 120 adds an amount of extra current to the second oscillator (and so changes its frequency) by an amount (between minimum and maximum values of the output saw-tooth waveform from the first oscillator 112) determined by the instant at which the transmission gate 120 is closed.

Thus, in order to obtain increased randomisation, the user 'blips' or 'pulses' the adjustment bit for the transmission gate 120 immediately before reading a random number from the random number generating arrangement 110.

It will be understood that because the frequency of the output saw-tooth waveform from the first oscillator 112 will typically vary with manufacturing process variations, with operating temperature changes and with operating voltage changes, and because the switching time of the transistors forming the transmission gate 120 will vary for the same reasons, the exact analogue value sampled and held on the storage capacitor 122 will not be predictable in practice. Further, it will be understood that the exact effect of this analogue value on changing the current produced by the current source 118 will also vary with manufacturing process variations, with operating temperature changes and with operating voltage changes to the transistors forming the current source 118. As a result of these compounded unpredictabilities, it will be appreciated that the exact effect of the adjustment caused such 'blipping' or 'pulsing' is highly unpredictable, and that such 'blipping' or 'pulsing therefore considerably increases the randomness of the resultant random number.

Practical analysis and testing of the arrangement of FIG. 2 has confirmed that the 'blipping' or 'pulsing' described produces a significant increase in randomness.

It will be appreciated that the first oscillator 112 may produce a varying waveform other than the saw-tooth waveform described (for example a continuously varying waveform such as a sine wave), but that periods of constancy in the waveform with may reduce the effectiveness of the increased randomisation produced by 'blipping' or 'pulsing' the adjustment bit for the transmission gate 120.

Claims

1. A random number generator arrangement comprising:

   first oscillator means for producing a varying waveform output signal at a first frequency;
   second oscillator means, coupled to the output of the first oscillator means so that the frequency of the second oscillator means is controlled by the output of the first oscillator means, for producing a pulse train output representative of a random number,
   characterised by
   adjustment means coupled between the output of the first oscillator means and the second oscillator means for adjusting by a variable amount the frequency of the second oscillator means.

2. A random number generator arrangement according to claim 1 wherein the second oscillator means includes a current source which is coupled to the output of the first oscillator means, and the adjustment means comprises storage means for storing the value of the output of the first oscillator means at a chosen time and for applying the stored value to the current source so that the frequency thereof is controlled by the combination of the output of the first oscillator means and the stored value.

3. A random number generator arrangement according to claim 2 wherein the storage means comprises a capacitor coupled to the output of the first oscillator means by a switch.

4. A random number generator arrangement according to claim 3 wherein the opening and closing of the switch is controlled by the value of a software settable data bit.

5. A random number generator arrangement according to any preceding claim further comprising means for selectably dividing the output from the second oscillator means.

6. A random number generator arrangement according to claim 5 wherein the division ratio of the divider means is controlled by the value of a software settable data bit.

7. A random number generator arrangement according to any preceding claim wherein the varying waveform produced by the first oscillator means is a substantially saw-tooth waveform.

8. A method of generating a random number comprising the steps of:

driving first oscillator means to produce a varying waveform output signal at a first frequency;

driving second oscillator means, coupled to the output of the first oscillator means so that the frequency of the second oscillator means is controlled by the output of the first oscillator means, to produce a pulse train output representative of a random number,

characterised by

sampling the output of the first oscillator means at a chosen point in time and adjusting the frequency of the second oscillator means by applying thereto the sampled value.

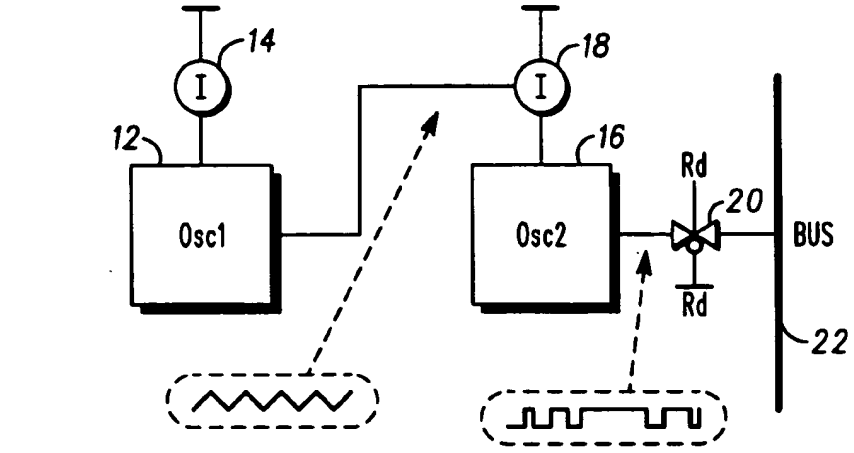

FIG.1
— PRIOR ART —

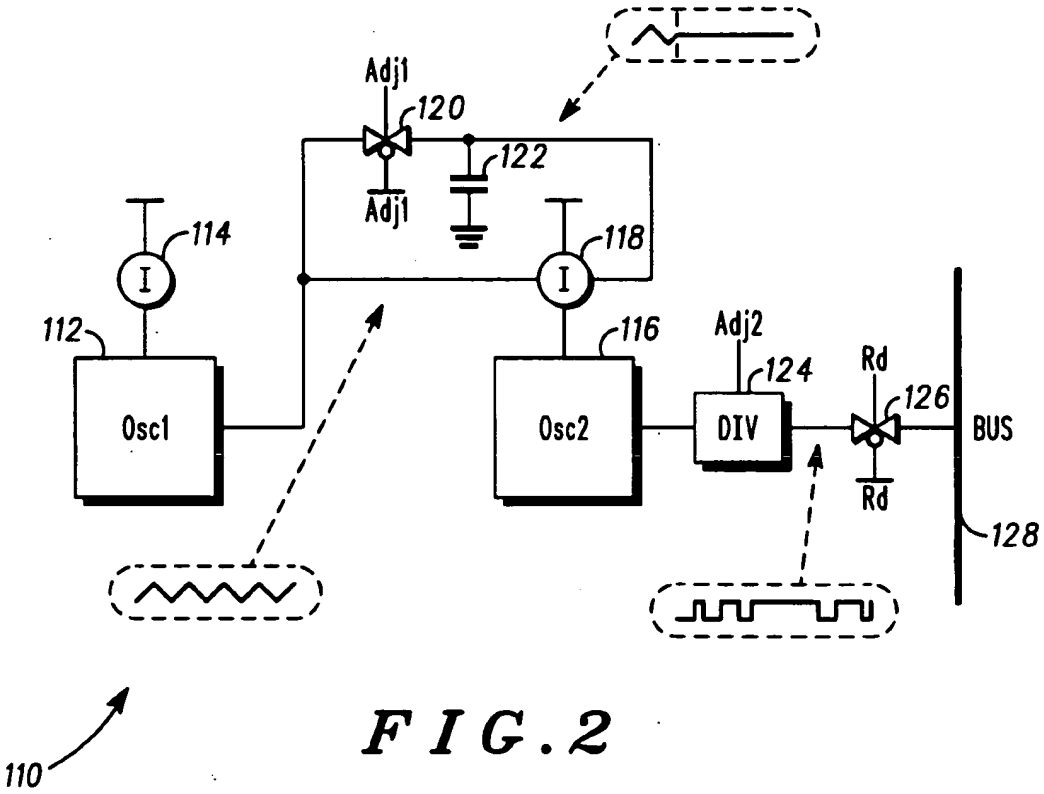

FIG.2